Towards Automatic Critical Infrastructure Protection through Machine Learning

Lorena Cazorla, Cristina Alcaraz, Javier Lopez

Network, Information and Computer Security (NICS) Lab,
University of Malaga, Spain
{lorena,alcaraz,jlm}@lcc.uma.es

Dated: April, 2015

Abstract

Critical Infrastructure Protection (CIP) faces increasing challenges in number and in sophistication, which makes vital to provide new forms of protection to face every day's threats. In order to make such protection holistic, covering all the needs of the systems from the point of view of security, prevention aspects and situational awareness should be considered. Researchers and Institutions stress the need of providing intelligent and automatic solutions for protection, calling our attention to the need of providing Intrusion Detection Systems (IDS) with intelligent active reaction capabilities. In this paper, we support the need of automating the processes implicated in the IDS solutions of the critical infrastructures and theorize that the introduction of Machine Learning (ML) techniques in IDS will be helpful for implementing automatic adaptable solutions capable of adjusting to new situations and timely reacting in the face of threats and anomalies. To this end, we study the different levels of automation that the IDS can implement, and outline a methodology to endow critical scenarios with preventive automation. Finally, we analyze current solutions presented in the literature and contrast them against the proposed methodology.

Keywords: Critical Infrastructure Protection, Machine Learning, Intrusion Detection.

1 Introduction

A control system (CS) is a device or set of devices that perform the management and the regulation of behavior of other devices or systems. Examples of such CS are supervisory control and data acquisition (SCADA) systems and distributed control systems (DCS). CS are deployed in multiple types of environments, but when they serve as assistance to infrastructures essential for the well being of the society, they are considered critical control systems, and their good functioning is of paramount importance.

In order to protect these systems, different organizations have developed guidelines of protection for the *Critical Infrastructures* (CI)([1] [2]), that manifest the need of offering advanced defense solutions for the CIs in the prevention area. One of the main pillars in this research is the dynamic prevention solutions, such as Intrusion Detection Systems (IDS) [3], capable of complementing prevention with automated action in crisis scenarios.

Traditionally IDS were designed for general-purpose networks, and their application for CIP is not always adequate due to the presence of strict requirements and property communication protocols in the CIs. However, the need of introducing such element in critical contexts has sound support of the scientific community [4] and the institutions [3]. What is more, according to [5] there is a great need for providing these IDS with intelligence and automatic capabilities, in order for them to respond rapidly and efficiently to emergency situations, especially in isolated scenarios. In this paper we therefore theorize that the application of ML techniques would help building the status of preparedness and response for the CIs, constructing intelligent protection systems that are capable of autonomously react against the threats posed to the CIs.

This paper is organized as follows: first we provide an introduction, in Section 2 the concept of automation in the field of detection for CIs is explained, discussing the main advantages of automation through ML. Section 3, provides an analysis of the state-of-the art solutions for IDS in CIP, classifying them according to the automation needs they cover. Finally, the conclusions of this study are provided and future work is outlined.

1.1 Machine Learning Techniques

Learning techniques are varied, and they originate from very different fields of knowledge (e.g. optimization, statistics, logic, etc.). It is interesting to study these methods taking into account characteristics that impose constraints to the underlying system and impact the possibility of introducing them in the context of CIP. It is important to discuss the *knowledge scheme* and the *level of supervision* of the system [6]. The knowledge scheme indicates the level of knowledge that is feed to the system prior to the training: *prior knowledge-based systems* are fed with the knowledge and experience of an expert, *prior knowledge free systems* are based on the knowledge extracted through an automatic (or semi-automatic) procedure of training, the *hybrid knowledge-based systems* add the knowledge of an expert to the model of the system obtained through training. The level of supervision of the system can be divided into: *supervised learning*, where the system has knowledge about the variables learned, and *unsupervised learning*, where no knowledge is provided to the system when training it [6].

According to the level of supervision or implication of the operator in the process of learning, it is possible to categorize the main ML techniques [7] that could result of use in the context of intrusion detection for CIP into *supervised* and *unsupervised* learning methods. In the first category, the main approaches are the *logic-based algorithms*, such as *decision trees*, *rule learners*; the *statistical learning algorithms*, such as the *Bayesian networks*, the *Naïve Bayes* and the *instance-based learners*; and the *artificial neural networks*, such as the *perceptron-based techniques*. Concerning the unsupervised learning methods, the main techniques are *association rule learning* (e.g.

Apriori algorithm and *FP-growth* algorithm), *clustering* techniques (e.g. the *k-means*), and the *Markov chains*. In Section 3 we will study the IDS solutions available in the literature, and which of these techniques they implement.

2 Levels of Automation of an IDS in CIP

Automation is defined as the introduction of automatic equipment or processes within a system, to assist or replace human operators, mostly when the tasks involved are intensive in computations or the working conditions are extreme. In CIP, there are subsystems that are usually deployed in distant and isolated locations, where the automation of the tasks is of paramount importance. In this context, there is a proven need [5] [8] of making certain processes automatic, and thus assisting the human operators in these complex tasks. Systems based on automatic methods will be capable of performing automatically, and will serve as powerful tools of *reaction*, providing methods of *prevention of cascading failures*, other than only detection of anomalies and intrusions.

When monitoring critical systems using ML techniques, the concept of automation can be split into four different dimensions: the *automation of the data collection and feeding*, the *automation of the learning process*, the *automation of the detection process*, and in several contexts [3], it is also vital to talk about the *automation of the reaction process*, when the IDS is capable of launching prevention mechanisms automatically as the first response against a detected threat or anomaly. Thus, we define the five levels of automation as a methodology to determine the degree of automation of an IDS:

- *Automation of the data collection*: the collection of the raw data is a process that is inherently automatic, since it involves capturing and recording vast amounts of data involving measurements, logs, etc. for later processing and training.

- *Automation of the data feeding*: comprises the preprocessing, normalizing and preparing the raw data to feed the inputs of the system. This process is difficult, costly and the majority of the real-life systems require the preprocessing of the data to be performed (semi-)manually. It is vital to provide automatic mechanisms with the object to adapt the functioning of ML-based system to face the real-life problems.

- *Automation of the learning process*: the learning process comprises three steps: *training*, *tuning* and *validation*. The training of the system is usually automatic, but the process of tuning and validation normally needs the participation of an operator in order to set the system to a correct functioning for a context. However, learning is performed before the deployment of the system, thus this kind of automation has less impact in the performance of the system.

- *Automation of the detection process*: is vital for the performance of the system, and it is usually referred to a deployed system that has to provide its services in real time. The need to tune the model in a later stage of the deployment of the system can impact negatively the performance of the system. In this case,

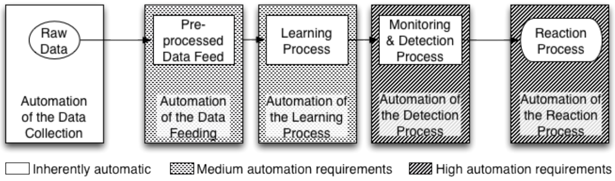
Raw Data
Pre-processed Data Feed
Learning Process
Monitoring & Detection Process
Reaction Process
Automation of the Data Collection
Automation of the Data Feeding
Automation of the Learning Process
Automation of the Detection Process
Automation of the Reaction Process
Inherently automatic
Medium automation requirements
High automation requirements

Figure 1: The needs of online automation of a critical IDS system

the need of automation is vital, and the tuning of the models should be at least semi-automatic.

- *Automation of the reaction process*: after detecting any anomaly or intrusion, the system must take appropriate actions to avoid the problem to escalate. According to its nature, the reaction can be: *passive reaction* and *active reaction*. Passive responses are typical in current IDS and include actions such as raising alarms or logging off the system [8]; active responses are those implemented to react against the anomaly or the intrusion in order to avoid the system failure. In CIP, monitoring systems have traditionally implemented passive reaction processes based on sending warnings to the operators and making available the information for them to fix the system. These solutions are mostly semi-automatic and highly dependent on the presence and accuracy of the operators. The scientific community need to focus in this dimension of the automation, to provide first response mechanisms to prevent failures to cascade through the critical systems in a rapid way [5].

Figure 1 shows the levels of automation of an IDS. For the sake of clarity it is represented as a line, but each step is a cycle of refinement itself. Here is stressed the need of online detection and reaction automation, understanding that preprocessing and learning processes can be performed offline without detriment to the IDS's behavior.

3 Analysis of the Current Literature

Learning techniques can be applied to a variety of systems that provide protection for the CI, particularly to IDS solutions [9] [10]. We have surveyed the literature in the search of solutions that provide IDS solutions for CIP, reviewing the characteristics and the degree of automation of each solution. For each of these systems, we analyze the levels of automation provided according to the classification in Section 2. We have summarized our analysis in Table 3, where we can distinguish three different dimensions, namely: *prior-knowledge scheme*, *supervision* and *automation*, that categorize the reviewed systems according to the classification established in this paper.

Düssel et al. [9] present a payload-based anomaly-based network IDS for CIs, capable of monitoring the traffic in real time. The IDS makes use of different techniques, the system extracts the information in the form of vectors, calculates the distance measures of similarity and compares them to a previously learned model of normality, indicating the presence or absence of an anomaly by raising alarms. Roosta et al. [8] introduce

Table 1: Review of several systems according to the automation and knowledge dimensions

System	Method	Prior Knowledge	Automation					Technique
			Data Collection	Preprocessing	Learning	Detection	Reaction	
[9]	Sup.	Free	Auto	No	Auto	Auto	Passive	Statistics, ML and Rules
[8]	Sup.	Required	N/A	N/A	N/A	N/A	N/A	Rules
[11]	Sup.	Free	Auto	No	Auto	Auto	Passive	Statistics
[12]	Unsup.	Mixed	Auto	No	Auto	Auto	N/A	Pattern Discovery
[13]	Sup.	Required	N/A	N/A	N/A	Auto	Passive	Rules
[14]	Sup.	Required	Auto	N/A	N/A	Auto	Passive	Rules, Statistics
[10]	Unsup.	Free	Auto	Auto	Auto	Auto	N/A	Statistics, ML and Rules
[15]	Sup.	Required	N/A	N/A	N/A	Auto	Passive	Rules, ML
[16]	N/A	Required	N/A	N/A	N/A	Auto	Passive	Specifications
[17]	Unsup.	Free	Auto	No	Auto	Auto	Passive	Clustering

an anomaly-based IDS for wireless process control systems. The IDS presented is theoretical, where the detection is based on expert-designed policy rules. Yang et al. [11] present and IDS based on pattern matching, capable of detecting anomalies by analyzing the deviation from normal behavior. They use autoassociative kernel regression models and a sequential probability ration test to discern an attack from the normal behavior. MELISSA [12] is a semantic-level IDS based on FP-Trees [7] that looks for undesirable user actions by processing logs in the SCADA control center. Carcano et al. [13] propose a state-based IDS that use rules to detect complex attack scenarios based on chains of illicit network packets. Autoscopy [14] is an IDS capable of detecting malware that tries to "hijack" pointers and routines of the system; first it learns the behavior of the system and during its operation, it uses statistics to discern anomalous behaviors and raise alarms. D'Antonio et al. present an IDS [10] that implements a rule learner to classify values into normal and attack data, it has a flow monitor component that extract statistical relations between different sessions to refine the learned model. Cheung et al. [15] propose a three-layer IDS that is based on models and patterns of the system designed by an expert. One of the layers implement a Bayesian learning module to detect changes in the availability of the surveilled system. Lin et al. [16] propose a specification-based IDS, that uses the formal specification of the system under surveillance to verify the correct use of the network packets. Raciti et al. present an IDS for Smart Grids [17] based on clustering techniques, for detecting anomalies in the cyber and the physical levels.

In Table 3 is interesting to observe that current systems implement only passive methods of reaction, they usually raise warnings to the operators, and they have to manually perform the inspections, repairs of the systems and help in crisis situations (e.g. voltage peaks in pylons, high pressures in dams, etc.). The main disadvantage of non-automatic systems is that help might arrive too late, and the failures of the system may cascade to other dependent systems, including other interdependent CIs, causing all kinds of havoc. Thus we find it vital that effective measures are taken, to avoid the possible social and economical harm derived from a cascading failure. There must be automatic active reaction processes, maybe based on ML techniques, that are capable of providing effective countermeasures in the face of any kind of anomaly or attack.

4 Conclusions

In this paper we support the need of implementing automatic and intelligent IDS in the CIs to create the state of readiness and prevention required by a CI. We defend that the introduction of ML for IDS can lead to autonomous systems capable of actively responding against the threats posed to a CI. To study the automation of IDS, we outline a methodology to evaluate the degree of automation of a given solution and stress the need of automation at the level of active reaction procedures against failures and intrusions. We discuss that the application of ML could be very beneficial to create IDS capable of reacting autonomously to threats. The need of automation has been contrasted with the current literature, describing the degree of automation of the reviewed solutions, and exposing the need of providing active reaction methods, intelligent enough to provide a safe layer of first response for CIs against threats. The methodology for automation and the revision of ML techniques for IDS in critical scenarios lays the foundations for future research and establishes the context for the design of IDS solutions that comply with the identified requirements of automation and intelligence.

Acknowledgments.

This work has been partially supported by the EU FP7 project FACIES (HOME/2011/CIPS/AG/4000002115), by the Spanish Ministry of Science and Innovation and FEDER (European Regional Development Fund) through the project SPRINT (TIN 2009 - 09237), and by the Andalusian government through the project PISCIS (P10-TIC-06334). Additionally, the second author has received funding from the Marie Curie COFUND programme "U-Mobility" co-financed by Universidad de Malaga and the European Community 7th PF under Grant Agreement No. 246550.

References

[1] European Commission: COM(2011) 163 Achievements and Next Steps: Towards Global Cyber-Security. Publications Office (2011)

[2] European Commission: COM(2009) 149 Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience. Publications Office (2009)

[3] Scarfone, K., Mell, P.: Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication **SP 800-94** (2012)

[4] Chertoff, M.: National Infrastructure Protection Plan. Department of Homeland Security (DHS), Washington, DC (2009)

[5] Alcaraz, C., Lopez, J.: Wide-Area Situational Awareness for Critical Infrastructure Protection. IEEE Computer **46**(4) (2013) 30–37

[6] Burbeck, K., Nadjm-Tehrani, S.: Adaptive Real-Time Anomaly Detection with Incremental Clustering. information security technical report **12**(1) (2007) 56–67

[7] Witten, I., Frank, E., Hall, M.: Data Mining: Practical Machine Learning Tools and Techniques: Practical Machine Learning Tools and Techniques. M. Kaufmann (2011)

[8] Roosta, T., Nilsson, D., Lindqvist, U., Valdes, A.: An Intrusion Detection System for Wireless Process Control Systems. In: Mobile Ad Hoc and Sensor Systems, 2008. MASS 2008. 5th IEEE International Conference on, IEEE (2008) 866–872

[9] Düssel, P., Gehl, C., Laskov, P., Bußer, J., Störmann, C., Kästner, J.: Cyber-Critical Infrastructure Protection using Real-Time Payload-Based Anomaly Detection. Critical Information Infrastructures Security (2010) 85–97

[10] D'Antonio, S., Oliviero, F., Setola, R.: High-Speed Intrusion Detection in Support of Critical Infrastructure Protection. Critical Information Infrastructures Security (2006) 222–234

[11] Yang, D., Usynin, A., Hines, J.: Anomaly-based Intrusion Detection for SCADA Systems. In: 5th Intl. Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies (NPIC&HMIT 05). (2006) 12–16

[12] Hadziosmanovic, D., Bolzoni, D., Hartel, P., Etalle, S.: MELISSA: Towards Automated Detection of Undesirable User Actions in Critical Infrastructures. (2011)

[13] Carcano, A., I.Fovino, Masera, M., Trombetta, A.: State-Based Network Intrusion Detection Systems for SCADA Protocols: a Proof of Concept. Critical Information Infrastructures Security (2010) 138–150

[14] Reeves, J., Ramaswamy, A., Locasto, M., Bratus, S., Smith, S.: Intrusion Detection for Resource-Constrained Embedded Control Systems in the Power Grid. International Journal of Critical Infrastructure Protection (2012)

[15] Cheung, S., Dutertre, B., Fong, M., Lindqvist, U., Skinner, K., Valdes, A.: Using Model-based Intrusion Detection for SCADA Networks. In: Proceedings of the SCADA Security Scientific Symposium. (2007) 127–134

[16] Lin, H., Slagell, A., Martino, C.D., Kalbarczyk, Z., Iyer, R.: Adapting Bro into SCADA: Building a Specification-based Intrusion Detection System for the DNP3 Protocol. (2012)

[17] Raciti, M., Nadjm-Tehrani, S.: Embedded Cyber-Physical Anomaly Detection in Smart Meters, Springer (2012)